

Amendments to the Specification:

Please replace the paragraph on page 1, lines 5 to 9, with the following rewritten paragraph:

The present invention relates to an apparatus and a method for computing the sum of a divisor $D_1 = \text{g.c.d.}((a_1(x)), (y - b_1(x)))$ and a divisor $D_2 = \text{g.c.d.}((a_2(x)), (y - b_2(x)))$ on jacobian of a hyperelliptic curve $y^2 + y = f(x)$ defined over $\text{GF}(2^n)$ (Galois Field of characteristic 2), where g.c.d. is greatest common divisor.

Please replace the paragraph on page 2, lines 2 to 13, with the following rewritten paragraph:

There is a field referred to as K , and its algebraically closed field is referred to as \bar{K} (K with a bar on it). A hyperelliptic curve C of genus g over K is defined by an equation of the form: $y^2 + h(x)y = f(x)$. Here, $h(x)$ is a polynomial of a degree g at most, and $f(x)$ is a monic polynomial of degree $2g+1$. Here, ~~polynomial~~ polynomials f and g have coefficients in K and curve C ~~have~~ has no singular points. Also, when rational point $P=(x,y)$ is given, its opposite point is defined as $\bar{P} = (x, -y - h(x))$ (\bar{P} is P with a bar on it). If P is infinite-point P_∞ , it shall be $P_\infty = \bar{P}_\infty$ (P_∞ is P_∞ with a bar on it). Hereafter, this application assumes a case of field $K = \text{GF}(2^n)$, $h(x)=1$.

Please replace the paragraph on page 2, lines 14 and 15, with the following rewritten paragraph:

A divisor D of C is a finite form sum of \bar{K} -points P_1, \dots, P_r and given by

Please replace the paragraph on page 2, line 16, with the following rewritten

paragraph:

$$\{\text{Expression 1}\} D = \sum_{P_i \in C} m_i P_i$$

Please replace the paragraph on page 3, line 1, with the following rewritten paragraph:

$$\{\text{Expression 2}\} D_1 = \sum_{P_i \in C} m_i P_i$$

Please replace the paragraph on page 3, line 2, with the following rewritten paragraph:

$$\{\text{Expression 3}\} D_2 = \sum_{P_i \in C} n_i P_i$$

Please replace the paragraph on page 3, line 4, with the following rewritten paragraph:

$$\{\text{Expression 4}\} D_1 + D_2 = \sum_{P_i \in C} (m_i + n_i) P_i$$

Please replace the paragraph on page 3, line 11, with the following rewritten paragraph:

$$\{\text{Expression 5}\} \text{div}(h) = \sum_{P_i \in C} \text{ord}_{P_i}(h) P_i = \sum m_i P_i - \sum n_i Q_i$$

Please replace the paragraph on page 4, line 17, with the following rewritten paragraph:

$$[\text{Expression 6}] D_1 = \sum_{P_i \in C} m_i P_i - \left(\sum_{P_i \in C} m_i \right) P_\infty$$

Please replace the paragraph on page 5, lines 2 and 3, with the following rewritten paragraph:

(2) If P_i appears in D_1 , then the point \bar{P}_i does not ~~P_i doesn't~~ appear as one of P_j ($j \neq i$).

Please replace the paragraph on page 5, line 4, with the following rewritten paragraph:

(3) When $P_i = \bar{P}_i$, $m_i = 1$ at most.

Please replace the paragraph on page 5, line 8, with the following rewritten paragraph:

$$[\text{Expression 7}] \sum_{P_i \in C} m_i \leq g$$